Available online at www.sciencedirect.com
ScienceDirect
Theoretical Computer Science 377 (2007) 93–109
Theoretical Computer Science
www.elsevier.com/locate/tcs

Classes of representable disjoint NP-pairs☆

Olaf Beyersdorff

Institut für Informatik, Humboldt-Universität zu Berlin, Germany

Received 3 August 2006; received in revised form 17 January 2007; accepted 4 February 2007

Communicated by A. Razborov

Abstract

For a propositional proof system P we introduce the complexity class DNPP(P) of all disjoint NP-pairs for which the disjointness of the pair is efficiently provable in the proof system P. We exhibit structural properties of proof systems which make canonical NP-pairs associated with these proof systems hard or complete for DNPP(P). Moreover, we demonstrate that non-equivalent proof systems can have equivalent canonical pairs and that depending on the properties of the proof systems different scenarios for DNPP(P) and the reductions between the canonical pairs exist.

Keywords: Disjoint NP-pairs; Propositional proof systems

1. Introduction

Disjoint NP-pairs (DNPP) have been introduced as a complexity-theoretical tool to model security aspects of public-key crypto systems [9,10]. Further, the theory of disjoint NP-pairs is intimately connected to propositional proof complexity with applications to automated theorem proving and lower bounds to the length of proofs [22,21, 14]. These applications attracted more complexity-theoretical research on the structure of the class of disjoint NP-pairs (cf. [11,6–8]).

Various disjoint NP-pairs have been defined from propositional proof systems which characterize properties of these proof systems. Razborov [22] was the first to associate a canonical pair with a proof system. This pair corresponds to the reflection property of the proof system. Pudlák [21] showed that also the automatizability of the proof system and the feasible interpolation property are expressible by disjoint NP-pairs. In this way disjoint NP-pairs have substantially contributed to the understanding of propositional proof systems.

Conversely, this paper aims to transfer proof-theoretical knowledge to the theory of NP-pairs to gain a more detailed understanding of the structure of the class of disjoint NP-pairs and in particular of the NP-pairs defined

☆ Preliminary versions of the results of this paper appeared in the proceedings of the conferences FSTTCS 2004 [O. Beyersdorff, Representable disjoint NP-pairs, in: Proc. 24th Conference on Foundations of Software Technology and Theoretical Computer Science, in: Lecture Notes in Computer Science, vol. 3328, Springer-Verlag, Berlin, Heidelberg, 2004, pp. 122–134] and TAMC 2006 [O. Beyersdorff, Disjoint NP-pairs from propositional proof systems, in: Proc. 3rd Conference on Theory and Applications of Models of Computation, in: Lecture Notes in Computer Science, vol. 3959, Springer-Verlag, Berlin, Heidelberg, 2006, pp. 236–247].

E-mail address: beyersdo@informatik.hu-berlin.de.

0304-3975/$ - see front matter
doi:10.1016/j.tcs.2007.02.005

from propositional proof systems. We investigate a slight modification of the first-order arithmetic representations of disjoint NP-pairs defined by Razborov [22]. We also define more general propositional representations for NP-pairs and associate with any propositional proof system P a subclass $\mathsf{DNPP}(P)$ of NP-pairs for which the disjointness is provable with short P-proofs. Somewhat surprisingly, under suitable conditions on P these non-uniform classes $\mathsf{DNPP}(P)$ equal their uniform versions which are defined via arithmetical representations.

Investigating the class $\mathsf{DNPP}(P)$ we show that under reasonable assumptions on the proof system P this class is closed under reductions for pairs and possesses hard or complete pairs in form of Razborov's canonical pair, Pudlák's interpolation pair and a third, new pair associated with the proof system. The properties of the classes $\mathsf{DNPP}(P)$ are decisively influenced by the closure properties of the underlying proof system. We demonstrate that proof systems P with different properties give rise to different scenarios for $\mathsf{DNPP}(P)$ and the reductions between the NP-pairs associated with P.

The mentioned closure properties are of logical nature: it should be feasible to carry out basic operations like modus ponens or substitutions by constants in the proof system. A recent result of Glaßer et al. [8] states that every DNPP is equivalent to the canonical pair of some proof system. However, the proof systems constructed for this purpose do not satisfy our regularity conditions. The observations of this paper indicate that the Cook-Reckhow framework of propositional proof systems might be too broad for the study of naturally defined classes of disjoint NP-pairs. It therefore seems to be natural to make additional assumptions on the properties of proof systems. Consequently, in our opinion, the canonical pairs of these natural proof systems deserve special attention.

Further, we investigate the connection between the simulation order of propositional proof systems and disjoint NP-pairs. As all information about the proof lengths is coded in the canonical pair the simulations between proof systems are reflected in reductions between NP-pairs and specifically between canonical pairs. Among other things this implies that the existence of optimal propositional proof systems implies the existence of complete NP-pairs. On the other hand this connection is not as tight as one might hope for. We provide different ways to construct non-equivalent proof systems with equivalent canonical pairs. A first example for this situation is due to Pudlák [21]. Here we search for general conditions on proof systems that yield a collapse between their canonical pairs. In particular, we analyse a weak notion of simulation for proof systems introduced in [15] but not much studied elsewhere. This simulation is provably weaker than the ordinary reduction between proof systems but is equivalent with respect to the existence of optimal proof systems. We show that all proof systems that are equivalent with respect to this weak simulation possess equivalent canonical pairs.

2. Proof systems with natural properties

Propositional proof systems were defined in a very general way by Cook and Reckhow in [5] as polynomial-time functions P which have as its range the set TAUT of all tautologies, which we consider in the language containing the connectives $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ and constants $\top$ and $\bot$. A string π with $P(\pi) = \varphi$ is called a P-proof of the tautology φ. By $P \vdash_{\leq m} \varphi$ we indicate that there is a P-proof of φ of size $\leq m$. If Φ is a set of propositional formulas we write $P \vdash_* \Phi$ if there is a polynomial p such that $P \vdash_{\leq p(|\varphi|)} \varphi$ for all $\varphi \in \Phi$. If $\Phi = \{\varphi_n \mid n \geq 0\}$ is a sequence of formulas we also write $P \vdash_* \varphi_n$ instead of $P \vdash_* \Phi$.

Proof systems are compared according to their strength by simulations, introduced in [5] and [15]. A proof system S *simulates* a proof system P (denoted by $P \leq S$) if there exists a polynomial p such that for all tautologies φ and P-proofs π of φ there is an S-proof π' of φ with $|\pi'| \leq p(|\pi|)$. If such a proof π' can even be computed from π in polynomial time we say that S *p-simulates* P and denote this by $P \leq_p S$. A proof system is called *(p-)optimal* if it (p-)simulates all proof systems. A system P is *polynomially bounded* if $P \vdash_*$ TAUT. By a theorem of Cook and Reckhow [5] polynomially-bounded proof systems exist if and only if $\mathsf{NP} = \mathsf{coNP}$.

In the following we will often consider proof systems satisfying some additional properties. We say that a proof system P is *closed under modus ponens* if there exists a constant c such that $P \vdash_{\leq m} \varphi$ and $P \vdash_{\leq n} \varphi \rightarrow \psi$ imply $P \vdash_{\leq m+n+|\psi|+c} \psi$ for all formulas φ and ψ. P is *closed under substitutions* if there exists a polynomial q such that $P \vdash_{\leq m} \varphi$ implies $P \vdash_{\leq q(m+|\sigma(\varphi)|)} \sigma(\varphi)$ for all formulas φ and all substitutions σ. Likewise we say that P is *closed under substitutions by constants* if there exists a polynomial q such that $P \vdash_{\leq m} \varphi(\bar{x}, \bar{y})$ implies $P \vdash_{\leq q(m)} \varphi(\bar{a}, \bar{y})$ for all formulas $\varphi(\bar{x}, \bar{y})$ and constants $\bar{a} \in \{0,1\}^{|\bar{x}|}$. A system P is *closed under disjunctions* if there is a polynomial q such that $P \vdash_{\leq m} \varphi$ implies $P \vdash_{\leq q(m+|\psi|)} \varphi \vee \psi$ for arbitrary formulas ψ. If these proof transformations can be executed in polynomial time, then we speak of *efficient* closure properties. The following property is shared by all

systems that simulate the truth-table system: a proof system *evaluates formulas without variables* if these formulas have polynomially long proofs.

We call a proof system *line based* if proofs in the system consist of sequences of formulas, and formulas in such a sequence are derived from earlier formulas in the sequence by the rules available in the proof system. Most of the studied proof systems like resolution, cutting planes and Frege systems are line based in this sense. The most interesting proof systems for us will be *Frege proof systems* F which are usual textbook proof systems based on axioms and rules. Enhancing F by the possibility to abbreviate complex formulas by propositional variables results in the *extended Frege proof system* EF (see e.g. [12]).

Line-based proof systems can be enhanced by additional axioms. We will do this in two different ways. Let Φ be a set of tautologies which can be decided in polynomial time. By $P + \Phi$ we denote the proof system P augmented by the possibility to use all formulas from Φ as axiom schemes. This means that formulas from Φ as well as substitution instances of these formulas can be freely introduced as new lines in $P + \Phi$-proofs. In contrast to this we use the notation $P \cup \Phi$ for the proof system that extends P by formulas from Φ as new axioms. The difference to $P + \Phi$ is that in $P \cup \Phi$ we are only allowed to use formulas from Φ but not their substitution instances in proofs.

We say that a line-based proof system P allows *efficient deduction* if there exists a polynomial p such that for all finite sets Φ of tautologies $P \cup \Phi \vdash_{\leq m} \psi$ implies $P \vdash_{\leq p(m+n)} (\bigwedge_{\varphi\in\Phi} \varphi) \to \psi$ where $n = |\bigwedge_{\varphi\in\Phi} \varphi|$. In particular, it is well known that this deduction property holds for Frege systems (see e.g. [12]):

Theorem 1 (*Deduction Theorem*). *Frege systems allow efficient deduction.*

A class of particularly well behaved proof systems is formed by proof systems which correspond to arithmetic theories. To explain this correspondence we have to translate first order arithmetic formulas into propositional formulas. Π_1^b-formulas have only bounded universal quantifiers and describe coNP-predicates. A Π_1^b-formula $\varphi(x)$ is translated into a sequence $\|\varphi(x)\|^n$ of propositional formulas containing one formula per input length for the number x such that $\varphi(x)$ is true if and only if $\|\varphi(x)\|^n$ is a tautology where $n = |x|$ (cf. [12]). We use $\|\varphi(x)\|$ to denote the set $\{\|\varphi(x)\|^n \mid n \geq 1\}$.

The *reflection principle* for a propositional proof system P states a strong form of the consistency of the proof system P. It is formalized by the $\forall\Pi_1^b$-formula

$$\mathrm{RFN}(P) = (\forall\pi)(\forall\varphi)\mathrm{Prf}_P(\pi, \varphi) \to \mathrm{Taut}(\varphi)$$

where Prf_P and Taut are suitable arithmetic formulas describing P-proofs and tautologies, respectively. The formulas Prf_P and Taut can be chosen such that Taut is a Π_1^b-formula, whereas Prf_P is provably equivalent in S_2^1 both to a Σ_1^b and a Π_1^b-formula (cf. [12]). A proof system P has the *reflection property* if $P \vdash_* \|\mathrm{RFN}(P)\|^n$ holds.

In [16] a general correspondence between arithmetic theories T and propositional proof systems P is introduced. Pairs (T, P) from this correspondence possess in particular the following two properties:

(1) Let $\varphi(x)$ be a Π_1^b-formula such that $T \vdash (\forall x)\varphi(x)$. Then there exists a polynomial-time computable function f that on input 1^n outputs a P-proof of $\|\varphi(x)\|^n$.
(2) P is the strongest system for which T proves the correctness, i.e., $T \vdash \mathrm{RFN}(P)$ and if $T \vdash \mathrm{RFN}(S)$ for a proof system S, then $S \leq_p P$.

In the following we call a proof system P *regular* if there exists an arithmetic theory T such that the properties 1 and 2 are fulfilled for (T, P). The most prominent example for this correspondence is the pair (S_2^1, EF).

In [12] a sequence of tautologies φ_n is called *hard for a proof system* P if φ_n is constructible in polynomial time and $P \nvdash_* \varphi_n$. By a theorem of [12] hard sequences exist for a proof system $P \geq EF$ if and only if P is not optimal.

3. NP-pairs defined from propositional proof systems

A pair (A, B) is called a disjoint NP-pair (DNPP) if $A, B \in \mathsf{NP}$ and $A \cap B = \emptyset$. A separator of (A, B) is a set C such that $A \subseteq C$ and $B \cap C = \emptyset$. If such a separator can be computed in polynomial time, then the pair is called *p-separable*.

Grollmann and Selman [9] defined the following *Turing reduction* between pairs: $(A, B) \leq_T (C, D)$, if there exists a polynomial-time oracle Turing machine M such that for every separator T of (C, D) $L(M^T)$ separates (A, B).

If for inputs from $A \cup B$ the machine M makes only queries to $C \cup D$ we call the reduction performed by M a *smart Turing reduction*.

The following more refined many-one reduction for pairs also stems from [9]: $(A, B) \leq_p (C, D)$ if there exists a polynomial-time computable function f such that $f(A) \subseteq C$ and $f(B) \subseteq D$. Because elements from $\overline{A \cup B}$ can be mapped to $C \cup D$ a reduction $(A, B) \leq_p (C, D)$ does not imply that A and B are many-one reducible to C and D, respectively. This is, however, the case for the following stronger reduction defined in [11]: $(A, B) \leq_s (C, D)$ if there exists a function $f \in \mathsf{FP}$ with $f^{-1}(C) = A$ and $f^{-1}(D) = B$. As usual we define the equivalence relation $\equiv_p$ as $(A, B) \equiv_p (C, D)$ if $(A, B) \leq_p (C, D)$ and $(C, D) \leq_p (A, B)$, and similarly for $\equiv_s$.

Razborov [22] associated a *canonical* disjoint NP-pair $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ with a proof system P where the first component $\mathrm{Ref}(P) = \{(\varphi, 1^m) | P \vdash_{\leq m} \varphi\}$ contains information about proof lengths in P, and $\mathrm{SAT}^* = \{(\varphi, 1^m) | \neg\varphi \in \mathrm{SAT}\}$ is a padded version of SAT. The canonical pair corresponds to the reflection principle of the proof system, but it is also linked to the automatizability of the proof system, a concept that is of great relevance for automated theorem proving. In [4] a proof system P is called *automatizable* if there exists a deterministic procedure that takes as input a formula φ and outputs a P-proof of φ in time polynomial in the length of the shortest P-proof of φ. This is equivalent to the existence of a deterministic polynomial-time algorithm that takes as input $(\varphi, 1^m)$ and produces a P-proof of φ if $(\varphi, 1^m) \in \mathrm{Ref}(P)$. From this reformulation of automatizability it is clear that automatizable proof systems have p-separable canonical pairs. The converse is probably not true as the following proposition shows.

Proposition 2. *There exists a proof system P that has a p-separable canonical pair. But P is not automatizable unless $\mathsf{P} = \mathsf{NP}$.*

Proof. We define the proof system P as follows:

$$P(\pi) = \begin{cases} \varphi & \text{if } \pi = (\varphi, 1^m),\ m \geq 2^{|\varphi|} \text{ and } \varphi \in \mathrm{TAUT} \\ \varphi \vee \top & \text{if } \pi = (\varphi, \alpha) \text{ and } \alpha \text{ is a satisfying assignment for } \varphi \\ \top & \text{otherwise.} \end{cases}$$

The following algorithm separates the canonical pair of P:

```
1  Input: (φ, 1^m)
2  IF φ = ψ ∨ ⊤ or φ = ⊤ THEN output 1
3  IF m ≥ 2^|φ| THEN
4    IF φ ∈ TAUT THEN output 1
5  output 0.
```

The test $\varphi \in \mathrm{TAUT}$ in line 4 can be performed in polynomial time by checking all assignments because the parameter m is big enough according to line 3.

If the input formula φ is a tautology, then the algorithm outputs 1 by lines 2 and 4, except for the case when φ is not of the form $\psi \vee \top$ and $m < 2^{|\varphi|}$. But in this case we have by definition $(\varphi, 1^m) \notin \mathrm{Ref}(P)$. Therefore $(\varphi, 1^m) \in \mathrm{SAT}^*$ always leads to the answer 0 whereas inputs $(\varphi, 1^m) \in \mathrm{Ref}(P)$ are always answered by 1.

The proof system P is not automatizable because this would mean that on input $\varphi \vee \top$ we would have to produce in polynomial time a satisfying assignment of φ provided $\varphi \in \mathrm{SAT}$. This implies in particular the existence of a deterministic polynomial-time algorithm to decide SAT and hence $\mathsf{P} = \mathsf{NP}$. □

This example is not entirely satisfactory as the proof system constructed in the last proof is not very natural. But it might be hard to prove Proposition 2 for natural proof systems as it is conjectured that the canonical pairs of all studied proof systems are not p-separable (cf. [21]). At least for proof systems stronger than bounded-depth Frege systems we have good reason to believe that their canonical pairs are not p-separable because cryptographic pairs reduce to the canonical pairs of these systems [17,4,2].

However, Pudlák showed in [21] that the canonical pair of a proof system P is p-separable if and only if there exists an automatizable proof system which simulates P. Therefore proof systems with p-separable canonical pair are called *weakly automatizable*.

Pudlák [21] also introduced the *interpolation pair* of a proof system:

$$I_1(P) = \{(\varphi, \psi, \pi) \mid \mathrm{Var}(\varphi) \cap \mathrm{Var}(\psi) = \emptyset,\ \neg\varphi \in \mathrm{SAT} \text{ and } P(\pi) = \varphi \vee \psi\}$$
$$I_2(P) = \{(\varphi, \psi, \pi) \mid \mathrm{Var}(\varphi) \cap \mathrm{Var}(\psi) = \emptyset,\ \neg\psi \in \mathrm{SAT} \text{ and } P(\pi) = \varphi \vee \psi\}$$

where $\mathrm{Var}(\varphi)$ denotes the set of variables occurring in φ. This pair is p-separable if and only if the proof system P has the efficient interpolation property. Efficient interpolation has been successfully used to show lower bounds to the proof size of a number of proof systems like resolution and cutting planes [3,13,19].

4. Representations of NP-pairs

In the previous section we briefly explained how properties of propositional proof systems can be captured by disjoint NP-pairs that are suitably defined from these proof systems. Conversely, we now employ proof-theoretical methods to gain a more detailed understanding of the class of disjoint NP-pairs. For this we need to represent arbitrary disjoint NP-pairs in propositional proof systems. This can be done uniformly in theories of bounded arithmetic or non-uniformly in propositional proof systems. We will start with the uniform concept which was first considered by Razborov [22].

Definition 3 (*Razborov [22]*). A Σ_1^b-formula φ is an *arithmetic representation* of an NP-set A if for all natural numbers a the formula $\varphi(a)$ is true if and only if $a \in A$.

A DNPP (A, B) is *representable* in an arithmetic theory T if there are Σ_1^b-formulas φ and ψ representing A and B, respectively, such that $T \vdash (\forall x)(\neg\varphi(x) \vee \neg\psi(x))$. By $\mathsf{DNPP}(T)$ we denote the class of all disjoint NP-pairs that are representable in T.

Since $(\forall x)(\neg\varphi(x) \vee \neg\psi(x))$ is a $\forall\Pi_1^b$-formula we can also express the disjointness of A and B propositionally by the sequence of tautologies $\|\neg\varphi(x) \vee \neg\psi(x)\|^n$. Hence propositional representations of disjoint NP-pairs can be simply obtained by transforming Definition 3 with the translation $\|.\|$ to the propositional level. However, we will give a more general definition. For this we first need to define a propositional encoding of NP-sets.

Definition 4. Let A be an NP-set over the alphabet $\{0, 1\}$. A *propositional representation* for A is a sequence of propositional formulas $\varphi_n(\bar{x}, \bar{y})$ with the following properties:

(1) $\varphi_n(\bar{x}, \bar{y})$ has propositional variables $\bar{x}$ and $\bar{y}$ such that $\bar{x}$ is a vector of n propositional variables.
(2) There exists a polynomial-time algorithm that on input 1^n outputs $\varphi_n(\bar{x}, \bar{y})$.
(3) Let $\bar{a} \in \{0, 1\}^n$. Then $\bar{a} \in A$ if and only if $\varphi_n(\bar{a}, \bar{y})$ is satisfiable.

Once we have a propositional description of NP-sets we can also represent disjoint NP-sets in propositional proof systems. This notion is captured by the next definition.

Definition 5. Let P be a propositional proof system. A disjoint NP-pair (A, B) is *representable in* P if there are propositional representations $\varphi_n(\bar{x}, \bar{y})$ of A and $\psi_n(\bar{x}, \bar{z})$ of B such that $\bar{x}$ are the common variables of $\varphi_n(\bar{x}, \bar{y})$ and $\psi_n(\bar{x}, \bar{z})$ and $P \vdash_* \neg\varphi_n(\bar{x}, \bar{y}) \vee \neg\psi_n(\bar{x}, \bar{z})$.

By $\mathsf{DNPP}(P)$ we denote the class of all disjoint NP-pairs which are representable in P.

In the class $\mathsf{DNPP}(P)$ we collect those NP-pairs for which the disjointness is efficiently provable in the proof system P. Clearly, considering stronger proof systems we expect this class to grow, namely, if P and Q are proof systems with $P \leq Q$, then $\mathsf{DNPP}(P) \subseteq \mathsf{DNPP}(Q)$.

We remark that the provability of the disjointness of a pair (A, B) in a proof system depends crucially on the choice of the representations for A and B.

Proposition 6. *If optimal proof systems do not exist, then the following holds: for every proof system P and for every disjoint* NP*-pair (A, B) there exist propositional representations φ_n for A and ψ_n for B such that P does not prove the disjointness of (A, B) with respect to these representations, i.e. $P \not\vdash_* \neg\varphi_n \vee \neg\psi_n$.*

Proof. Let the pair (A, B) be representable in the proof system P via the representations φ_n' and ψ_n', i.e. $P \vdash_* \neg\varphi_n' \vee \neg\psi_n'$. By Q we denote the proof system $EF + \|\mathrm{RFN}(P)\|$. By assumption Q is not optimal, hence we get a sequence τ_n of hard tautologies for Q. We define $\varphi_n(\bar{x}, \bar{y}, \bar{u}) = \varphi_n'(\bar{x}, \bar{y}) \vee \neg\tau_n(\bar{u})$ and $\psi_n(\bar{x}, \bar{z}, \bar{v}) = \psi_n'(\bar{x}, \bar{z}) \vee \neg\tau_n(\bar{v})$

where all tuples of variables $\bar{x}$, $\bar{y}$, $\bar{z}$, $\bar{u}$ and $\bar{v}$ are pairwise disjoint. As $\neg\tau_n(\bar{u})$ is not satisfiable $\varphi'_n(\bar{x},\bar{y}) \vee \neg\tau_n(\bar{u})$ represents A. Similarly, ψ_n is a propositional representation for B. But Q and hence also P does not prove the disjointness of A and B with respect to the representations φ_n and ψ_n. Assume on the contrary that $Q \vdash_* \neg\varphi_n \vee \neg\psi_n$. By definition this means

$$Q \vdash_* \neg(\varphi'_n(\bar{x},\bar{y}) \vee \neg\tau_n(\bar{u})) \vee \neg(\psi'_n(\bar{x},\bar{z}) \vee \neg\tau_n(\bar{v})).$$

Using basic manipulations of formulas, which can be efficiently performed in Q, we get polynomial-size Q-proofs of $\tau_n(\bar{u})$, contradicting the choice of τ_n as hard tautologies for Q. □

Let us give a concrete example for this situation. The Clique-Coloring pair (CC_0, CC_1) takes inputs of the form (G, k), where the first component contains graphs G with a clique of size k, whereas graphs in CC_1 are $k-1$-colourable. Pudlák [20] shows that the disjointness of (CC_0, CC_1) is not provable with polynomial-size proofs in the cutting planes system CP for some canonical representations of the components CC_0 and CC_1. On the other hand, the Clique-colouring pair is p-separable as shown by Lovász [18]. Hence (CC_0, CC_1) is contained in $\mathsf{DNPP}(CP)$ as the following argument shows. We choose some simple p-separable pair (A, B) that is representable in CP. As all p-separable are equivalent we can reduce (CC_0, CC_1) to (A, B). The class $\mathsf{DNPP}(CP)$ is closed under $\leq_p$-reductions (we will show this in Section 5, Theorem 8). Therefore we get $(CC_0, CC_1) \in \mathsf{DNPP}(CP)$ which means that there exist polynomial-size CP-proofs for the disjointness of the Clique-colouring pair for suitable representations of its components.

Now we will compare the uniform and non-uniform representations.

Theorem 7. *Let $P \geq EF$ be a regular proof system which is closed under substitutions by constants and let $T \supseteq S^1_2$ be a theory corresponding to P. Then $\mathsf{DNPP}(P) = \mathsf{DNPP}(T)$.*

Proof. For the first inclusion let (A, B) be a disjoint NP-pair in $\mathsf{DNPP}(P)$ and let $\varphi_n(\bar{x},\bar{y})$ and $\psi_n(\bar{x},\bar{z})$ be propositional representations for A and B, respectively, such that $P \vdash_* \neg\varphi_n(\bar{x},\bar{y}) \vee \neg\psi_n(\bar{x},\bar{z})$.

Because P is closed under substitutions by constants there exists a polynomial p such that for all $\bar{a} \in \{0,1\}^n$ we have $P \vdash_{\leq p(n)} \neg\varphi_n(\bar{a},\bar{y}) \vee \neg\psi_n(\bar{a},\bar{z})$. Assume further that the polynomial-time computable functions f and g generate the formulas φ_n and ψ_n, i.e., $f(1^n) = \varphi_n(\bar{x},\bar{y})$ and $g(1^n) = \psi_n(\bar{x},\bar{z})$. Consider the first-order formula

$$\varphi(\alpha) = \mathit{Assign}(\alpha,\bar{x}) \wedge \neg\mathrm{Taut}(\neg f(1^{|\alpha|})(\alpha(\bar{x}),\bar{y})),$$

where $\mathit{Assign}(\alpha,\bar{x})$ describes that α codes a propositional assignment to the variables $\bar{x}$ and Taut is the Π^b_1-formula from $\mathrm{RFN}(P)$ (cf. [12] for details on propositional encodings). As the above notation is still not completely precise, let us explain how to understand the definition of φ. At input $1^{|\alpha|}$ the function f outputs the formula $\varphi_{|\alpha|}(\bar{x},\bar{y})$. In φ the computation of f is expressed by a Σ^b_1-formula. Then we use again the free variable α of φ to obtain a propositional assignment to the propositional variables $\bar{x}$. The formula $\neg\mathrm{Taut}(\neg f(1^{|\alpha|})(\alpha(\bar{x}),\bar{y}))$ is a Σ^b_1-formulation for the satisfiability of $\varphi_{|\alpha|}(\bar{x},\bar{y})$, where the variables $\bar{x}$ are substituted by the constants specified in α, and only the variables $\bar{y}$ remain free.

The above explanation shows that φ is a Σ^b_1-formula. Moreover, it is clear that φ represents A. Similarly, we define a representation for B as:

$$\begin{aligned}\psi(\alpha) \;=\; & \mathit{Assign}(\alpha,\bar{x}) \wedge \neg\mathrm{Taut}(\neg g(1^{|\alpha|})(\alpha(\bar{x}),\bar{z})) \wedge \\ & (\exists\pi)|\pi| \leq p(|\alpha|) \wedge \mathrm{Prf}_P(\pi, \neg f(1^{|\alpha|})(\alpha(\bar{x}),\bar{y}) \vee \neg g(1^{|\alpha|})(\alpha(\bar{x}),\bar{z})).\end{aligned}$$

In order to verify that T can prove the disjointness of A and B with respect to the above representations, assume that M is a model of T and $\alpha \in M$ is an element such that $M \models \psi(\alpha)$. In particular this means that there exists an element $\pi \in M$ such that

$$M \;\models\; \mathrm{Prf}_P(\pi, \neg f(1^{|\alpha|})(\alpha(\bar{x}),\bar{y}) \vee \neg g(1^{|\alpha|})(\alpha(\bar{x}),\bar{z})).$$

Because $T \vdash \mathrm{RFN}(P)$ this implies

$$M \;\models\; \mathrm{Taut}(\neg f(1^{|\alpha|})(\alpha(\bar{x}),\bar{y}) \vee \neg g(1^{|\alpha|})(\alpha(\bar{x}),\bar{z})).$$

The theory $T \supseteq S_2^1$ is strong enough to prove Tarski's truth conditions for the propositional satisfaction relation $\models$ (cf. [12] Lemma 9.3.9). In particular T proves that a tautological disjunction of formulas without common variables contains at least one tautological disjunct, and hence we get

$$M \models \mathrm{Taut}(\neg f(1^{|\alpha|})(\alpha(\bar{x}), \bar{y})) \vee \mathrm{Taut}(\neg g(1^{|\alpha|})(\alpha(\bar{x}), \bar{z})).$$

But $M \models \psi(\alpha)$ implies $M \models \mathrm{Taut}(\neg f(1^{|\alpha|})(\alpha(\bar{x}), \bar{y}))$, and therefore $M \not\models \varphi(\alpha)$. Hence we have shown $T \vdash (\forall x)\neg\varphi(x) \vee \neg\psi(x)$.

To show $\mathsf{DNPP}(T) \subseteq \mathsf{DNPP}(P)$ let φ and ψ be Σ_1^b-formulas representing A and B, respectively, such that $T \vdash (\forall x)\neg\varphi(x) \vee \neg\psi(x)$. We define the propositional representations of A and B as the $\|.\|$-translations of φ and ψ, namely:

$$\varphi_n(\bar{x}, \bar{y}) = \|\varphi(x)\|^n \quad \text{and} \quad \psi_n(\bar{x}, \bar{z}) = \|\psi(x)\|^n$$

where we choose the auxiliary variables $\bar{y}$ of $\|\varphi(x)\|^n$ and $\bar{z}$ of $\|\psi(x)\|^n$ disjoint. These sequences can be generated in polynomial time and represent A and B. Because the formula $(\forall x)\neg\varphi(x) \vee \neg\psi(x)$ is a $\forall\Pi_1^b$-formula, we derive $P \vdash_* \|\neg\varphi(x) \vee \neg\psi(x)\|^n$, implying $P \vdash_* \neg\varphi_n \vee \neg\psi_n$. □

At first sight Theorem 7 might come as a surprise as it states that the non-uniform and uniform concepts equal when representing disjoint NP-pairs in regular proof systems. The uniform representations of NP-pairs are translated via $\|.\|$ to non-uniform representations in a straightforward manner. For the transformation of propositional representations into first-order formulas it is, however, essential to change the representation of one of the components.

5. The complexity class DNPP(P)

The aim of this section is to show that the subclasses $\mathsf{DNPP}(P)$ of disjoint NP-pairs are indeed examples for well defined complexity classes. We will provide justification for this claim by demonstrating that the classes $\mathsf{DNPP}(P)$ are closed under reductions and also possess hard or complete pairs for well defined proof systems P.

We start by giving sufficient conditions for the closure of $\mathsf{DNPP}(P)$ under $\leq_p$ (and hence also under $\leq_s$). Translating the reductions to the propositional level we have to work with uniform circuit families computing the reduction functions. Since it is possible in resolution to prove the uniqueness of circuit computations we can show the following:

Theorem 8. *Let P be a proof system which simulates resolution and is closed under disjunctions. Then $\mathsf{DNPP}(P)$ is closed under $\leq_p$.*

Proof. Let (A, B) and (C, D) be disjoint NP-pairs. Let (C, D) be representable in P, i.e., there exist representations $\varphi_n(\bar{x}, \bar{y})$ and $\psi_n(\bar{x}, \bar{z})$ of C and D, respectively, such that $P \vdash_* \neg\varphi_n(\bar{x}, \bar{y}) \vee \neg\psi_n(\bar{x}, \bar{z})$. Assume further that (A, B) is $\leq_p$-reducible to (C, D) via the polynomial-time computable function f. We have to show that also (A, B) is representable in P. For this we fix arbitrary representations $\chi_n(\bar{x}, \bar{r})$ and $\theta_n(\bar{x}, \bar{s})$ for A and B, respectively. Without loss of generality we may assume that the reduction function f generates on inputs of length n outputs of length exactly $p(n)$ for some fixed polynomial p. Let $C_n : \{0,1\}^n \to \{0,1\}^{p(n)}$ be a uniform circuit family which computes the function f. The computation of the circuits C_n can be described by propositional formulas $C_n(\bar{x}, \bar{p}, \bar{u})$ which state that on input corresponding to the propositional variables $\bar{x}$ the circuit produces the output corresponding to $\bar{p}$. The variables $\bar{u}$ are auxiliary variables for the gates of the circuit.

Consider the sequence of propositional formulas:

$$\varphi'_n = \chi_n(\bar{x}, \bar{r}) \wedge C_n(\bar{x}, \bar{p}, \bar{u}) \wedge \varphi_{p(n)}(\bar{p}, \bar{y}).$$

The formulas φ'_n provide a propositional representation of the set A because they propositionally express that $\bar{x} \in A$ and there exists a computation of C_n on input $\bar{x}$ that outputs an element from the set C. Similarly, the sequence

$$\psi'_n = \theta_n(\bar{x}, \bar{s}) \wedge C_n(\bar{x}, \bar{q}, \bar{v}) \wedge \psi_{p(n)}(\bar{q}, \bar{z})$$

represents B. We have to check that P proves the disjointness of A and B with respect to φ'_n and ψ'_n. The P-proof proceeds along the following lines. By hypothesis we have polynomial-size P-proofs for the formulas

$$\neg\varphi_{p(n)}(\bar{p}, \bar{y}) \vee \neg\psi_{p(n)}(\bar{p}, \bar{z}). \tag{1}$$

By induction on the number of gates of a circuit we can show that resolution proves the uniqueness of computations of Boolean circuits in polynomial-size resolution proofs. Because P simulates resolution this means that we have polynomial-size P-proofs of the formulas:

$$C_n(\bar{x}, \bar{p}, \bar{u}) \wedge C_n(\bar{x}, \bar{q}, \bar{v}) \to (\bar{p} \leftrightarrow \bar{q}). \tag{2}$$

From (1) and (2) we obtain polynomial-size P-proofs of

$$C_n(\bar{x}, \bar{p}, \bar{u}) \wedge C_n(\bar{x}, \bar{q}, \bar{v}) \to \neg\varphi_{p(n)}(\bar{p}, \bar{y}) \vee \neg\psi_{p(n)}(\bar{q}, \bar{z}),$$

from which we obtain by closure under disjunctions polynomial-size P-proofs of the disjointness of A and B with respect to the propositional representations φ'_n and ψ'_n. Hence $(A, B) \in \mathsf{DNPP}(P)$. □

Next we show the hardness of the canonical pair of a proof system P for the class $\mathsf{DNPP}(P)$.

Theorem 9. *Let P be a proof system that is closed under substitutions by constants and modus ponens and can evaluate formulas without variables. Then* $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ *is $\leq_p$-hard for* $\mathsf{DNPP}(P)$.

Proof. Let (A, B) be a DNPP and let $\varphi_n(\bar{x}, \bar{y})$ and $\psi_n(\bar{x}, \bar{z})$ be propositional representations of A and B, respectively, such that $P \vdash_* \neg\varphi_n(\bar{x}, \bar{y}) \vee \neg\psi_n(\bar{x}, \bar{z})$. Then the reduction $(A, B) \leq_p (\mathrm{Ref}(P), \mathrm{SAT}^*)$ is given by

$$a \mapsto (\neg\psi_{|a|}(\bar{a}, \bar{z}), 1^{p(|a|)})$$

for some suitable polynomial p. To see the correctness of the reduction let first be $a \in A$. Then there exists a witness $\bar{b}$ such that $\models \varphi_{|a|}(\bar{a}, \bar{b})$. From the P-proof of $\neg\varphi_{|a|}(\bar{x}, \bar{y}) \vee \neg\psi_{|a|}(\bar{x}, \bar{z})$ we get by substituting $\bar{a}$ for $\bar{x}$ and $\bar{b}$ for $\bar{y}$ a polynomially longer P-proof of $\neg\varphi_{|a|}(\bar{a}, \bar{b}) \vee \neg\psi_{|a|}(\bar{a}, \bar{z})$. $\neg\varphi_{|a|}(\bar{a}, \bar{b})$ is a false propositional formula without free variables and hence can be refuted with polynomial-size P-proofs. An application of modus ponens gives a P-proof of $\neg\psi_{|a|}(\bar{a}, \bar{z})$ as desired.

Assume now $a \in B$. Then $\neg\neg\psi_{|a|}(\bar{a}, \bar{z}) \equiv \psi_{|a|}(\bar{a}, \bar{z})$ is satisfiable and hence $(\neg\psi_{|a|}(\bar{a}, \bar{z}), 1^{p(|a|)}) \in \mathrm{SAT}^*$. □

Now we turn to proof systems which have the reflection property. The link between the canonical pair and the reflection property is already apparent from the definition of $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ and is also discussed in [21]. Using our terminology from Section 4 we may phrase this connection precisely as:

Proposition 10. *Let P be a proof system. Then P has the reflection property if and only if the canonical pair of P is representable in P with respect to the standard representations of* $\mathrm{Ref}(P)$ *and* SAT^**, which are obtained from the* $\|.\|$*-translations of the first-order formulas* $(\exists\pi)\ |\pi| \leq m \wedge \mathrm{Prf}_P(\pi, \varphi)$ *for* $\mathrm{Ref}(P)$ *and* $(\exists\alpha)\ |\alpha| \leq |\varphi| \wedge \alpha \models \neg\varphi$ *for* SAT^*.

From this we immediately conclude with Theorem 9:

Corollary 11. *Let P be a proof system that has the reflection property. Assume further that P is closed under substitutions by constants and modus ponens and can evaluate formulas without variables. Then* $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ *is $\leq_p$-complete for* $\mathsf{DNPP}(P)$.

In particular, this corollary holds for extension $EF + \|\Phi\|$ of EF by polynomial-time decidable sets Φ of true Π_1^b-formulas.

In this context it is natural to ask whether the canonical pair of the resolution calculus *Res* is $\leq_p$-complete for $\mathsf{DNPP}(Res)$. In view of Corollary 11 and the above discussion knowing whether $(\mathrm{Ref}(Res), \mathrm{SAT}^*)$ is representable in resolution would answer this question. Atserias and Bonet [1] proved that resolution does not have the reflection property. By Proposition 10 this means that the disjointness of $(\mathrm{Ref}(Res), \mathrm{SAT}^*)$ is not provable in resolution with respect to the standard representation. However, we cannot exclude the possibility that we have short resolution proofs of the disjointness of $(\mathrm{Ref}(Res), \mathrm{SAT}^*)$ with respect to some other representation. At least we can remark that, unless the canonical pair of resolution is p-separable, these proofs would have to be essentially non-uniform.

Proposition 12. *If the canonical pair of resolution is not p-separable, then there do not exist proofs for the disjointness of* $(\mathrm{Ref}(Res), \mathrm{SAT}^*)$ *that can be generated in polynomial time.*

Proof. Assume on the contrary that $\varphi(\bar{x}, \bar{y})$ and $\psi(\bar{x}, \bar{z})$ are representations of Ref(Res) and SAT*, respectively, such that we can generate resolution proofs of $\neg\varphi(\bar{x}, \bar{y}) \vee \neg\psi(\bar{x}, \bar{z})$ in polynomial time. Because resolution has the feasible interpolation property [13] this gives a polynomial-time computable algorithm that on input 1^n produces a circuit $C_n(\bar{x})$ such that $C_n(\bar{a}) = 1$ if $\varphi(\bar{a}, \bar{y})$ is satisfiable, and $C_n(\bar{a}) = 0$ in case of the satisfiability of $\psi(\bar{a}, \bar{z})$. As φ and ψ are representations for Ref(Res) and SAT*, respectively, this means that by evaluating the circuit C_n we get a separator for (Ref(Res), SAT*). Hence the canonical pair of resolutions is p-separable. □

6. The class DNPP(P) under the strong $\leq_s$-reduction

In this section we will analyse the class DNPP(P) under the strong reduction $\leq_s$. This is interesting because Glaßer, Selman, and Sengupta [6] proved that $\leq_s$ is indeed a proper refinement of $\leq_p$, provided that P $\neq$ NP. We start by associating to every proof system P a disjoint NP-pair $(U_1(P), U_2)$:

$$U_1(P) = \{(\varphi, \psi, 1^m) \mid \mathrm{Var}(\varphi) \cap \mathrm{Var}(\psi) = \emptyset,\ \neg\varphi \in \mathrm{SAT} \text{ and } P \vdash_{\leq m} \varphi \vee \psi\}$$
$$U_2 = \{(\varphi, \psi, 1^m) \mid \mathrm{Var}(\varphi) \cap \mathrm{Var}(\psi) = \emptyset \text{ and } \neg\psi \in \mathrm{SAT}\}.$$

In the following we will simply refer to this pair as the U-pair. The U-pair is reminiscent of the interpolation pair $(I_1(P), I_2(P))$, the essential difference being that $(I_1(P), I_2(P))$ contains actual P-proofs while $(U_1(P), U_2)$ contains only information on their lengths. In the following we will show that both these pairs have similar function for DNPP(P) under $\leq_s$ as the canonical pairs have under the weaker reduction $\leq_p$. But before we come to this we need to compare $(U_1(P), U_2)$ with the canonical pair of P.

Proposition 13. (1) *Let P be a proof system that is closed under disjunctions. Then* (Ref(P), SAT*) $\leq_p$ $(U_1(P), U_2)$.
(2) *Let P be a proof system that is closed under substitutions by constants and modus ponens and evaluates formulas without variables. Then we have* $(U_1(P), U_2) \leq_p$ (Ref(P), SAT*).

Proof. The first reduction is given by $(\varphi, 1^m) \mapsto (\bot, \varphi, 1^{p(m)})$, while the second reduction is performed by $(\varphi, \psi, 1^m) \mapsto (\psi, 1^{q(m)})$, where p and q are suitable polynomials depending on the proof system P. □

The following is an analogue of Theorem 9 for the strong reduction $\leq_s$.

Theorem 14. *Let P be a proof system that is closed under substitutions by constants. Then $(U_1(P), U_2)$ is $\leq_s$-hard for* DNPP(P).

Proof. Let (A, B) be a DNPP and let $\varphi_n(\bar{x}, \bar{y})$ and $\psi_n(\bar{x}, \bar{z})$ be propositional representations of A and B, respectively, such that $P \vdash_* \neg\varphi_n(\bar{x}, \bar{y}) \vee \neg\psi_n(\bar{x}, \bar{z})$. We claim that there exists a polynomial p such that

$$a \mapsto (\neg\varphi_{|a|}(\bar{a}, \bar{y}), \neg\psi_{|a|}(\bar{a}, \bar{z}), 1^{p(|a|)})$$

realizes a $\leq_s$-reduction from (A, B) to $(U_1(P), U_2)$.

Let first a be an element from A of length n. Because $\varphi_n(\bar{x}, \bar{y})$ represents A the formula $\varphi_n(\bar{a}, \bar{y})$ is satisfiable. As P is closed under substitutions by constants we have

$$P \vdash_{\leq p(n)} \neg\varphi_n(\bar{a}, \bar{y}) \vee \neg\psi_n(\bar{a}, \bar{z})$$

for the appropriate polynomial p. This confirms that a is mapped to $U_1(P)$. Similarly, elements from B are mapped to U_2. The reduction is strong, because if $a \notin A \cup B$, then neither $\varphi_{|a|}(\bar{a}, \bar{y})$ nor $\psi_{|a|}(\bar{a}, \bar{z})$ is satisfiable and hence $(\neg\varphi_{|a|}(\bar{a}, \bar{z}), \neg\psi_{|a|}(\bar{a}, \bar{z}), 1^{p(|a|)}) \notin U_1(P) \cup U_2$. □

As in the case of $\leq_p$ we can improve this hardness result to a completeness result for proof systems which have the reflection property. For proof systems P corresponding to theories of bounded arithmetic we can additionally prove the $\leq_s$-completeness of the interpolation pair of P for DNPP(P):

Theorem 15. *Let $P \geq EF$ be a regular proof system that is efficiently closed under substitutions by constants. Then $(U_1(P), U_2)$ and $(I_1(P), I_2(P))$ are $\leq_s$-complete for* DNPP(P). *In particular we have $(U_1(P), U_2) \equiv_s (I_1(P), I_2(P))$.*

Proof. To show that the pairs $(U_1(P), U_2)$ and $(I_1(P), I_2(P))$ are contained in $\mathsf{DNPP}(P)$, let $T \supseteq S_2^1$ be the theory corresponding to P. It is straightforward to show that the interpolation and the U-pair are representable in T via some standard representations using the formulas Prf_P and Taut. From this the representability of the pairs in P follows by Theorem 7.

Together with the $\leq_s$-hardness of $(U_1(P), U_2)$ for $\mathsf{DNPP}(P)$ as shown in Theorem 14 this yields the $\leq_s$-completeness of $(U_1(P), U_2)$.

To prove the $\leq_s$-hardness of $(I_1(P), I_2(P))$ for $\mathsf{DNPP}(P)$ let (A, B) be a disjoint NP-pair that is representable in P. By Theorem 7 we know that (A, B) is also representable in the theory T corresponding to P. Let $\varphi(x)$ and $\psi(x)$ be representations of A and B, respectively, such that $T \vdash (\forall x)\neg\varphi(x) \vee \neg\psi(x)$. Because P is regular there exists a polynomial-time computable function f that on input 1^n produces a P-proof of $\|\neg\varphi(x) \vee \neg\psi(x)\|^n$. Further, because by assumption P is efficiently closed under substitutions by constants we can use f to obtain a polynomial-time computable function g that on input $\bar{a} \in \{0,1\}^n$ outputs a P-proof of

$$\|\neg\varphi(x) \vee \neg\psi(x)\|^n(\bar{p}^x/\bar{a}),$$

where the variables $\bar{p}^x$ corresponding to x are replaced by the bits $\bar{a}$ of the number a. We claim that the $\leq_s$-reduction from (A, B) to $(I_1(P), I_2(P))$ is given by

$$a \mapsto (\|\neg\varphi(x)\|^{|a|}(\bar{p}^x/\bar{a}), \|\neg\psi(x)\|^{|a|}(\bar{p}^x/\bar{a}), g(\bar{a}))$$

where the auxiliary variables of $\|\neg\varphi(x)\|^{|a|}$ and $\|\neg\psi(x)\|^{|a|}$ are chosen disjoint. Verifying the correctness of the reduction proceeds as in Theorem 14. □

The equivalence of the interpolation pair and the U-pair for strong systems as stated in the last corollary might come unexpected as the first idea for a reduction from the U-pair to the I-pair probably is to generate proofs for $\varphi \vee \psi$ at input $(\varphi, \psi, 1^m)$. This, however, is not possible for extensions of EF, because a $\leq_p$-reduction from $(U_1(P), U_2)$ to $(I_1(P), I_2(P))$ of the form $(\varphi, \psi, 1^m) \mapsto (\varphi, \psi, \pi)$ implies the automatizability of the system P. But it is known that automatizability fails for strong systems $P \geq EF$ under cryptographic assumptions [17,21].

Clearly, for all proof systems $(\varphi, \psi, \pi) \mapsto (\varphi, \psi, 1^{|\pi|})$ computes a $\leq_p$-reduction from $(I_1(P), I_2(P))$ to $(U_1(P), U_2)$. For weak systems like resolution or cutting planes the opposite reduction is not possible unless the system is weakly automatizable. This is the content of the next proposition.

Proposition 16. *Let P be a proof system that has the feasible interpolation property and is closed under disjunctions. Then $(U_1(P), U_2) \leq_p (I_1(P), I_2(P))$ implies that P is weakly automatizable.*

Proof. Pudlák [21] showed that feasible interpolation for P means that the interpolation pair of P is p-separable. Therefore $(U_1(P), U_2) \leq_p (I_1(P), I_2(P))$ implies that also $(U_1(P), U_2)$ is p-separable. Closure of P under disjunctions together with Proposition 13 guarantees that $(\mathrm{Ref}(P), \mathrm{SAT}^*) \leq_p (U_1(P), U_2)$, hence also the canonical pair of P is p-separable and therefore P is weakly automatizable by a result from [21]. □

7. NP-pairs and the simulation order of proof systems

Now we use the results of the last sections to make some observations about the connection between the simulation order of proof systems and disjoint NP-pairs. As this analysis frequently involves proof systems with suitable closure properties which we want to avoid to list at each occasion we make the following definition:

Definition 17. We call a proof system P *strong* if $P \geq EF$ is a regular proof system that is closed under modus ponens and disjunctions and efficiently closed under substitutions by constants.

For instance, all extensions of EF by translations of true arithmetic formulas are strong in this sense, and therefore every proof system is simulated by some strong system. If we are interested in exploring optimal proof systems, then it is anyway legitimate to make as many assumptions on the systems as necessary. In particular, it is not difficult to show that optimal proof systems are strong.

We start our analysis with an easy but very useful observation from [21] expressing that the simulation order of propositional proof systems is reflected in reductions between the canonical pairs.

Proposition 18 (*Pudlák [21]*). *If P and S are proof systems with $P \leq S$, then we have* $(\mathrm{Ref}(P), \mathrm{SAT}^*) \leq_p (\mathrm{Ref}(S), \mathrm{SAT}^*)$.

Proof. The reduction is given by $(\varphi, 1^m) \mapsto (\varphi, 1^{p(m)})$ where p is the polynomial from $P \leq Q$. □

Probably not unexpected, this link between simulations of propositional proof systems and reductions between disjoint NP-pairs extends to the question of the existence of maximal elements in the respective orders. The following theorem which is usually attributed to Razborov [22] expresses this for the reduction $\leq_p$. Actually, the result as such is not stated in [22], but it easily follows from the results proven there.

Theorem 19 (*Razborov [22]*). *If P is an optimal proof system, then the canonical pair of P is a $\leq_p$-complete disjoint* NP*-pair.*

Proof. Let the proof system P be optimal and let (A, B) be some disjoint NP-pair. We choose arbitrary representations φ_n and ψ_n for A and B, respectively. Now we construct some strong proof system that admits polynomial-size proofs of $\neg\varphi_n \vee \neg\psi_n$. For example, $Q = EF + \{\neg\varphi_n \vee \neg\psi_n \mid n \geq 0\}$ is such a proof system. By Theorem 9 we get $(A, B) \leq_p (\mathrm{Ref}(Q), \mathrm{SAT}^*)$. Because P is optimal we have $Q \leq P$ and hence by Proposition 18 we get $(\mathrm{Ref}(Q), \mathrm{SAT}^*) \leq_p (\mathrm{Ref}(P), \mathrm{SAT}^*)$. Combining these reductions we get the reduction from (A, B) to the canonical pair of P, as claimed. □

Even without assuming the existence of optimal proof systems we can say that candidates for $\leq_p$-complete NP-pairs come from canonical pairs of strong proof systems:

Proposition 20. *Let (A, B) be $\leq_p$-complete for the class of all DNPP. Then we have $(A, B) \equiv_p (\mathrm{Ref}(P), \mathrm{SAT}^*)$ for some strong proof system P.*

Proof. As in the last proof we choose some strong proof system Q such that (A, B) is representable in Q. Then $(A, B) \leq_p (\mathrm{Ref}(Q), \mathrm{SAT}^*)$ and by assumption $(\mathrm{Ref}(Q), \mathrm{SAT}^*) \leq_p (A, B)$. □

We now analyse how the simulation order of proof systems is reflected in the more refined reduction $\leq_s$. In [6] it was shown that the reductions $\leq_p$ and $\leq_s$ are different under the assumption $\mathsf{P} \neq \mathsf{NP}$. Still we have:

Proposition 21. *Let P be a strong proof system. Then for all disjoint* NP*-pairs (A, B) we have $(A, B) \leq_p (U_1(P), U_2)$ if and only if $(A, B) \leq_s (U_1(P), U_2)$.*

Proof. Let $(A, B) \leq_p (U_1(P), U_2)$. Because P is strong, the pair $(U_1(P), U_2)$ is representable in P by Theorem 15. Again, as P is strong, P is closed under disjunctions and $P \geq EF$, hence in particular P simulates resolution. Thus we can deduce by Theorem 8 that also (A, B) is representable in P, from which we conclude with Theorem 14 $(A, B) \leq_s (U_1(P), U_2)$.

The opposite implication holds by definition. □

Corollary 22. *Let P and S be strong proof systems. Then we have* $(\mathrm{Ref}(P), \mathrm{SAT}^*) \leq_p (\mathrm{Ref}(S), \mathrm{SAT}^*)$ *if and only if* $(U_1(P), U_2) \leq_s (U_1(S), U_2)$.

Proof. For the first direction we get from

$$(U_1(P), U_2) \leq_p (\mathrm{Ref}(P), \mathrm{SAT}^*) \leq_p (\mathrm{Ref}(S), \mathrm{SAT}^*) \leq_p (U_1(S), U_2)$$

together with the last proposition $(U_1(P), U_2) \leq_s (U_1(S), U_2)$.

The other implication follows by combining the chain of reductions $(\mathrm{Ref}(P), \mathrm{SAT}^*) \leq_p (U_1(P), U_2) \leq_p (U_1(S), U_2) \leq_p (\mathrm{Ref}(S), \mathrm{SAT}^*)$. □

This yields an analogue of Proposition 18 for strong proof systems:

Corollary 23. *If P and S are strong proof systems with $P \leq S$, then we have $(U_1(P), U_2) \leq_s (U_1(S), U_2)$.*

Köbler, Messner, and Torán [11] proved that the existence of an optimal proof system implies the existence of $\leq_s$-complete NP-pairs. This result also follows from our observations here. Additionally, we can exhibit a complete pair:

Theorem 24. *If P is an optimal proof system, then $(U_1(P), U_2)$ is $\leq_s$-complete for the class of all DNPP.*

Proof. Let P be an optimal proof system and (A, B) a DNPP. We choose arbitrary propositional representations φ_n and ψ_n for A and B, respectively. As the sequence $\neg\varphi_n \vee \neg\psi_n$ is constructible in polynomial time there exists some proof system with polynomial-size proofs of these tautologies. Because P is optimal we also have polynomial-size P-proofs of $\neg\varphi_n \vee \neg\psi_n$, hence (A, B) is representable in P. The system P is optimal, so in particular it is strong. Therefore we can apply Theorem 15 to conclude $(A, B) \leq_s (U_1(P), U_2)$. □

We now turn again to the question whether complete pairs exists, but without assuming the existence of optimal proof systems. Glaßer, Selman, and Sengupta [6] proved that up to smart Turing reductions the answer to the problem does not depend on the strength of the reductions used. Here we give an easy proof based on our results from this section.

Theorem 25 (*Glaßer, Selman, Sengupta [6]*). *The class of all disjoint* NP*-pairs contains a $\leq_p$-complete pair if and only if it contains a $\leq_s$-complete pair.*

Proof. For the first direction we can assume with Proposition 20 that the $\leq_p$-complete DNPP has the form $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ for some strong proof system P. Then all disjoint NP-pairs are representable in P by Theorem 8, and therefore by Theorem 14 all DNPP are $\leq_s$-reducible to $(U_1(P), U_2)$.

The other direction holds by definition. □

In [6] Glaßer et al. prove that the existence of a complete DNPP under smart Turing reductions already implies the existence of a $\leq_p$-complete pair. We can easily re-prove their result in our framework by noticing:

Lemma 26. *Let $T \supseteq S_2^1$ be an L-theory. Then the class* DNPP(T) *is closed under smart Turing reductions.*

Proof. Let the pair (A, B) be smartly Turing reducible to (C, D) via the deterministic oracle Turing machine M, and let (C, D) be representable in T. Consider the NP-sets:

$$A' = \{x \mid x \in A \text{ and } M(x) \text{ accepts}\}$$
$$B' = \{x \mid x \in B \text{ and } M(x) \text{ rejects}\}.$$

By "$M(x)$ accepts" we mean that M accepts the input x by a computation where all oracle queries that are positively answered are verified by a computation of a nondeterministic machine for C and all negative answers are verified by D. Since the reduction is smart we have $A = A'$ and $B = B'$. For $T \vdash A' \cap B' = \emptyset$ it suffices to show in T the uniqueness of the computation of M on inputs x from $A \cup B$. Because T is an extension of S_2^1 it can prove the uniqueness of computations of the deterministic machine M, and the possibility to answer an oracle query both positively and negatively is excluded by $T \vdash C \cap D = \emptyset$. □

From this we conclude:

Proposition 27. *Suppose (A, B) is a smart $\leq_T$-complete pair. Let $T \supseteq S_2^1$ be an arithmetic theory in which (A, B) is representable. Then the pair $(U_1(P), U_2)$ is $\leq_s$-complete for all DNPP where P is the proof system corresponding to T.*

Proof. We choose arithmetical representations φ and ψ of A and B, respectively, and define the theory T as $S_2^1 + \neg\varphi \vee \neg\psi$. Then by the last lemma all DNPP are representable in T. By Theorem 7 this implies that all pairs are representable in the proof system $P = EF + \|\neg\varphi \vee \neg\psi\|$ and therefore the pair $(U_1(P), U_2)$ is $\leq_s$-complete by Theorem 14. □

It is not clear whether the class of pairs representable in some theory T is also closed under $\leq_T$-reductions. This corresponds to the open problem from [6] whether the existence of a $\leq_T$-complete pair implies the existence of a $\leq_p$-complete DNPP.

8. A weak reduction between proof systems

Besides $\leq$ and $\leq_p$ we can also study weaker reductions for propositional proof systems. In [15] a weak reduction $\leq'$ is defined between proof systems P and Q as follows: $P \leq' Q$ holds if for all polynomials p there exists a

polynomial q such that $P \vdash_{\leq p(|\varphi|)} \varphi$ implies $Q \vdash_{\leq q(|\varphi|)} \varphi$ for all tautologies φ. Using the notation $\vdash_*$ which hides the actual polynomials we can also express the reduction $\leq'$ more compactly as: $P \leq' Q$ if and only if for all sets Φ of tautologies $P \vdash_* \Phi$ implies $Q \vdash_* \Phi$.

Let us try to motivate the above definition. If we express combinatorial principles in propositional logic we arrive at collections Φ of tautologies that typically contain one tautology per input length. We say that a proof system P proves a combinatorial principle if there exist polynomially long P-proofs of the corresponding collection of tautologies. If $P \leq Q$, then every principle that is provable in P is also provable in Q. The Q-proofs are allowed to be longer than the P-proofs but only up to fixed polynomial amount independent of the principle proven. The reduction $\leq'$ is more flexible as it allows a different polynomial increase for each principle.

It is clear from the above explanation that $\leq$ is a refinement of $\leq'$. We observe that it is indeed a proper refinement, i.e. we can separate $\leq$ and $\leq'$. It is, however, not possible to achieve this separation with regular proof systems.

Proposition 28. (1) *Let P be a proof system that is not polynomially bounded. Then there exists a proof system Q such that $P \leq' Q$ but $P \not\leq Q$.*
(2) *Let Φ and Ψ be polynomial-time decidable sets of tautologies. Then $EF + \Phi \leq' EF + \Psi$ implies $EF + \Phi \leq EF + \Psi$.*

Proof. To prove part 1 let P be a proof system that is not polynomially bounded. We define the system Q. Q-proofs consist of multiple copies of P-proofs where the number of copies depends on the length of the P-proof, more precisely $Q(\pi) = \varphi$ if there exists a P-proof π' of φ such that $\pi = (\pi')^l$ where the number l of the copies of π' is determined as follows. Let k be a number such that $|\varphi|^{k-1} \leq |\pi'| < |\varphi|^k$. Then l is chosen as $l = |\varphi|^{(k-1)k}$. Hence we have:

$$|\varphi|^{k-1}|\varphi|^{(k-1)k} = |\varphi|^{k^2-1} \leq |\pi| < |\varphi|^k|\varphi|^{(k-1)k} = |\varphi|^{k^2}.$$

P is $\leq'$-simulated by Q because for each polynomial p majorized by n^k we can choose q as n^{k^2}, i.e., $P \vdash_{\leq|\varphi|^k} \varphi$ implies $Q \vdash_{\leq|\varphi|^{k^2}} \varphi$. But if P is not polynomially bounded, then for each k there exist formulas φ requiring P-proofs π' of lengths $> |\varphi|^k$, and hence $|\varphi|^{k^2-1} \leq |\pi|$ forces a super-polynomial increase in the proof length in the transformation from P-proofs π' into Q-proofs π. Hence there is no polynomial q such that $P \vdash_{\leq m} \varphi$ implies $Q \vdash_{\leq q(m)} \varphi$, i.e. $P \not\leq Q$.

Now we prove part 2. Let Φ and Ψ be polynomial-time decidable sets of tautologies. Let us denote the systems $EF + \Phi$ and $EF + \Psi$ by P and Q, respectively. The regularity of P implies $P \vdash_* \|\mathrm{RFN}(P)\|^n$. Because $P \leq' Q$ we also have $Q \vdash_* \|\mathrm{RFN}(P)\|^n$. This implies $P \leq Q$, as claimed. □

However, Krajíček and Pudlák [15] proved that the reductions $\leq$ and $\leq'$ are equivalent with respect to the existence of optimal proof systems.

9. Proof systems with equivalent canonical pairs

Already in Section 7 we have used the close relation between the simulation order of proof systems and the reductions between canonical pairs. Essentially, this connection rests upon the fact that $\mathsf{DNPP}(P)$ is a subclass of $\mathsf{DNPP}(Q)$ if the proof systems P is simulated by the system Q. For the canonical pairs this is expressed by the observation from Proposition 18 that a simulation of P by Q implies a $\leq_p$-reduction from the canonical pair of P to the canonical pair of Q.

We will now explore how tight the connection between the simulation order of proof systems and reductions in the lattice of pairs really is, i.e. to what extent the opposite implication of Proposition 18 is valid. If $P \not\leq Q$, then we cannot hope to reduce $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ to $(\mathrm{Ref}(Q), \mathrm{SAT}^*)$ by a reduction of the form $(\varphi, 1^m) \mapsto (\varphi, 1^n)$ that changes only the proof length but leaves the formula unchanged. However, unlike in the case of simulations between proof systems the reductions between canonical pairs have the flexibility to change the formula.

The aim of this section is to provide different techniques for the construction of non-equivalent proof systems with equivalent canonical pairs. One such example is given by Pudlák in [21] where he shows that two versions of the cutting planes proof system CP which do not $\leq$-simulate each other have $\leq_p$-equivalent canonical pairs. Here we search for general conditions on proof systems which imply the equivalence of the canonical pairs. The first condition will be the $\leq'$-equivalence of the proof systems. For this we show an analogue of Proposition 18 for $\leq'$.

Proposition 29. *Let P be a proof system that is closed under disjunctions and let Q be a proof system such that $P \leq' Q$. Then* $(\mathrm{Ref}(P), \mathrm{SAT}^*) \leq_p (\mathrm{Ref}(Q), \mathrm{SAT}^*)$.

Proof. We claim that for some suitable polynomial q the mapping

$$(\varphi, 1^m) \mapsto (\varphi \vee \bot^m, 1^{q(m)})$$

performs the desired $\leq_p$-reduction where $\bot^m$ stands for $\bot \vee \cdots \vee \bot$ (m disjuncts). To see this let first $(\varphi, 1^m) \in \mathrm{Ref}(P)$. Because P is closed under disjunctions there exists a polynomial p such that $P \vdash_{\leq m} \varphi$ implies $P \vdash_{\leq p(m)} \varphi \vee \bot^m$. Because of $P \leq' Q$ there is a polynomial q such that $Q \vdash_{\leq q(m)} \varphi \vee \bot^m$, i.e. $(\varphi \vee \bot^m, 1^{q(m)}) \in \mathrm{Ref}(Q)$.

If $(\varphi, 1^m) \in \mathrm{SAT}^*$, then the satisfiability of $\neg\varphi$ is transferred to $\neg(\varphi \vee \bot^m) \equiv \neg\varphi \wedge \top \wedge \cdots \wedge \top$. □

Combining Propositions 28 and 29 we get the afore mentioned counterexamples to the converse of Proposition 18.

Corollary 30. *Let P be a proof system that is closed under disjunctions and is not polynomially bounded. Then there exists a proof system Q such that $P \not\equiv Q$ and* $(\mathrm{Ref}(P), \mathrm{SAT}^*) \equiv_p (\mathrm{Ref}(Q), \mathrm{SAT}^*)$.

The proof systems P and Q from the last corollary have equivalent canonical pairs and are also $\leq'$-equivalent. Moreover, Proposition 29 implies that the $\leq_p$-degree of the canonical pair is already determined by the $\leq'$-degree of the system:

Corollary 31. *Let P and Q be $\leq'$-equivalent proof systems that are closed under disjunctions. Then* $(\mathrm{Ref}(P), \mathrm{SAT}^*) \equiv_p (\mathrm{Ref}(Q), \mathrm{SAT}^*)$.

Nevertheless we can also construct proof systems that have equivalent canonical pairs but are not $\leq'$-equivalent. We show this in the next theorem.

Theorem 32. *Let P be a line-based proof system that allows efficient deduction and let Φ be a sparse set of tautologies that can be decided and generated in polynomial time. Then* $(\mathrm{Ref}(P), \mathrm{SAT}^*) \equiv_p (\mathrm{Ref}(P \cup \Phi), \mathrm{SAT}^*)$.

Proof. As P is simulated by $P \cup \Phi$ we get $(\mathrm{Ref}(P), \mathrm{SAT}^*) \leq_p (\mathrm{Ref}(P \cup \Phi), \mathrm{SAT}^*)$.

Now we describe the converse reduction. Let p be the polynomial from the efficient deduction property of P. Because Φ is a sparse set there exists a polynomial q such that for each number m the set Φ contains at most $q(m)$ tautologies of length $\leq m$. Let $\Phi_m = \Phi \cap \Sigma^{\leq m}$ be the set of these tautologies.

Then $(\mathrm{Ref}(P \cup \Phi), \mathrm{SAT}^*)$ reduces to $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ via the function

$$(\psi, 1^m) \mapsto \left(\left(\bigwedge_{\varphi \in \Phi_m} \varphi \right) \to \psi, 1^{p(mq(m)+m)} \right).$$

To verify the claim assume that $(\psi, 1^m) \in \mathrm{Ref}(P \cup \Phi)$. Let π be a $P \cup \Phi$-proof of ψ of length $\leq m$. This proof π can use only formulas of length $\leq m$ from Φ of which there are only $\leq q(m)$ many. Hence the tautologies used in the proof π are contained in $\bigwedge_{\varphi \in \Phi_m} \varphi$. Therefore we know that π is also a proof for ψ in the proof system $P \cup \Phi_m$. Using the efficient deduction property of P we get a P-proof of size $\leq p(mq(m) + m)$ of $(\bigwedge_{\varphi \in \Phi_m} \varphi) \to \psi$.

Now assume $(\psi, 1^m) \in \mathrm{SAT}^*$. Then $\neg\psi$ is satisfiable. Therefore, also the formula $(\bigwedge_{\varphi \in \Phi_m} \varphi) \wedge \neg\psi$ is satisfiable because $\bigwedge_{\varphi \in \Phi_m} \varphi$ is a tautology. Hence the image of $(\psi, 1^m)$ is contained in SAT^*. □

If we start with a well defined line-based system P, then also $P \cup \Phi$ will have good properties (it will lose closure under substitutions). Hence both P and $P \cup \Phi$ can be chosen to satisfy a reasonable amount of the normality conditions of Section 2. As for any non-optimal proof system there exists a sequence of hard tautologies Φ which separates P and $P \cup \Phi$ with respect to $\leq'$, we obtain:

Corollary 33. *For any non-optimal line-based proof system P with efficient deduction there exists a sparse set Φ of tautologies that can be decided and generated in polynomial time such that $P \cup \Phi \not\leq' P$ and* $(\mathrm{Ref}(P), \mathrm{SAT}^*) \equiv_p (\mathrm{Ref}(P \cup \Phi), \mathrm{SAT}^*)$.

Because F admits efficient deduction (Theorem 1) we can formulate the following corollary:

Corollary 34. *Let Φ be a sparse set of tautologies that can be decided and generated in polynomial time. Then we have* $(\mathrm{Ref}(F), \mathrm{SAT}^*) \equiv_p (\mathrm{Ref}(F \cup \Phi), \mathrm{SAT}^*)$.

Table 1
The class $\mathsf{DNPP}(P)$ for different types of proof systems

Weak systems P	resolution, cutting planes
$(\mathrm{Ref}(P), \mathrm{SAT}^*)$	$\leq_p$-hard for $\mathsf{DNPP}(P)$
$(U_1(P), U_2)$	$\leq_s$-hard for $\mathsf{DNPP}(P)$
$(I_1(P), I_2(P))$	p-separable [21]
Reductions	$(I_1(P), I_2(P)) \leq_p (U_1(P), U_2) \equiv_p (\mathrm{Ref}(P), \mathrm{SAT}^*)$
	$(U_1(P), U_2) \not\leq_p (I_1(P), I_2(P))$ unless P is weakly automatizable
	closure of $\mathsf{DNPP}(P)$ under $\leq_p$ and $\leq_s$
Properties	closed under modus ponens and substitutions by constants
	efficient interpolation [13], no reflection for resolution [1]
Strong systems P	extensions $EF + \|\Phi\|$ of EF by polynomial-time computable sets of true Π_1^b-formulas Φ
$(\mathrm{Ref}(P), \mathrm{SAT}^*)$	$\leq_p$-complete for $\mathsf{DNPP}(P)$
$(U_1(P), U_2)$	$\leq_s$-complete for $\mathsf{DNPP}(P)$
$(I_1(P), I_2(P))$	$\leq_s$-complete for $\mathsf{DNPP}(P)$
Reductions	$(I_1(P), I_2(P)) \equiv_s (U_1(P), U_2) \equiv_p (\mathrm{Ref}(P), \mathrm{SAT}^*)$
	closure of $\mathsf{DNPP}(P)$ under smart $\leq_T$, $\leq_p$ and $\leq_s$
Properties	efficiently closed under modus ponens and substitutions
	no efficient interpolation under cryptographic assumptions [17]
	reflection property [16], regular
Other systems P	extensions $F \cup \Phi$ of F by suitable choices of polynomial-time constructible sets $\Phi \subseteq \mathrm{TAUT}$
$(\mathrm{Ref}(P), \mathrm{SAT}^*)$	not $\leq_p$-hard for $\mathsf{DNPP}(P)$, unless $(\mathrm{Ref}(F), \mathrm{SAT}^*)$ is $\leq_p$-complete for all DNPP
Reductions	$(I_1(P), I_2(P)) \leq_p (U_1(P), U_2)$, $(\mathrm{Ref}(P), \mathrm{SAT}^*) \leq_p (U_1(P), U_2)$
	$\mathsf{DNPP}(P)$ is not closed under $\leq_p$, unless $(\mathrm{Ref}(F), \mathrm{SAT}^*)$ is $\leq_p$-complete for all DNPP
Properties	closed under modus ponens
	not closed under substitutions by constants, unless $(\mathrm{Ref}(F), \mathrm{SAT}^*)$ is $\leq_p$-complete for all DNPP

10. Different scenarios for $\mathsf{DNPP}(P)$

In Section 5 we showed that the canonical pair of a proof system P is $\leq_p$-hard for $\mathsf{DNPP}(P)$ provided that the system P has sufficient closure properties. In the next theorem we give examples for proof systems P where the canonical pair of P is not hard for $\mathsf{DNPP}(P)$. Proving such a result requires a suitable hypothesis as $\mathsf{P} = \mathsf{NP}$ for example implies that all pairs with nonempty components are $\leq_p$-complete for the class of all DNPP. Here the assumption is that the canonical pair of F is not $\leq_p$-complete, and this assumption even characterizes the assertion.

Theorem 35. *There exists a sparse polynomial-time constructible set Φ of tautologies such that the canonical pair of $F \cup \Phi$ is not $\leq_p$-hard for the class $\mathsf{DNPP}(F \cup \Phi)$ if and only if $(\mathrm{Ref}(F), \mathrm{SAT}^*)$ is not $\leq_p$-complete for all pairs.*

Proof. For the first direction assume that for some sparse polynomial-time constructible set $\Phi \subseteq \mathrm{TAUT}$ the canonical pair of $F \cup \Phi$ is not $\leq_p$-hard for $\mathsf{DNPP}(F \cup \Phi)$. Then there exists a disjoint NP-pair (A, B) that is not $\leq_p$-reducible to the canonical pair of $F \cup \Phi$. By Corollary 34 we know that the canonical pairs of F and $F \cup \Phi$ are $\leq_p$-equivalent. Therefore $(A, B) \not\leq_p (\mathrm{Ref}(F), \mathrm{SAT}^*)$ and hence the canonical pair of F is not $\leq_p$-complete.

For the opposite direction assume that F is not $\leq_p$-complete. Then there exists a disjoint NP-pair (A, B) such that $(A, B) \not\leq_p (\mathrm{Ref}(F), \mathrm{SAT}^*)$. We choose some representations φ_n and ψ_n of A and B, respectively, and define the system P as $P = F \cup \{\neg\varphi_n \vee \neg\psi_n \mid n \geq 0\}$. By definition we have $P \vdash_* \neg\varphi_n \vee \neg\psi_n$, hence (A, B) is representable in P. By Corollary 34 we have $(\mathrm{Ref}(F), \mathrm{SAT}^*) \equiv_p (\mathrm{Ref}(P), \mathrm{SAT}^*)$. Hence $(A, B) \leq_p (\mathrm{Ref}(P), \mathrm{SAT}^*)$ would imply $(A, B) \leq_p (\mathrm{Ref}(F), \mathrm{SAT}^*)$ in contradiction to our assumption. □

In Table 1 we summarize some of the results for the class $\mathsf{DNPP}(P)$ for some typical proof systems P. This comparison demonstrates that proof systems P with different properties give rise to different scenarios for $\mathsf{DNPP}(P)$ and the reductions between the NP-pairs associated with P.

Some interesting questions are still unanswered by Table 1. For instance, how do $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ and $(U_1(P), U_2)$ compare with respect to the strong reduction $\leq_s$? At least for regular systems we know that $(\mathrm{Ref}(P), \mathrm{SAT}^*) \leq_s (U_1(P), U_2)$. Since $U_1(P)$ is NP-complete the NP-completeness of $\mathrm{Ref}(P)$ is a necessary condition for the opposite reduction to exist. To determine the complexity of $\mathrm{Ref}(P)$ for natural proof systems seems to be an interesting open problem. Approaching this question we note the following:

Proposition 36. (1) *For every proof system P that is closed under disjunctions there is a proof system P' with $P' \equiv_p P$ such that* $\mathrm{Ref}(P')$ *is* NP*-complete.*
(2) *On the other hand there are proof systems P and P' such that $P \equiv_p P'$ and* $\mathrm{Ref}(P)$ *is decidable in polynomial time while* $\mathrm{Ref}(P')$ *is* NP*-complete.*

Proof. To show part 1 of the proposition let P be a proof system that is closed under disjunctions. Closure under disjunctions implies in particular the existence of polynomial-size proofs of all formulas of the form $\varphi \vee \top$ for arbitrary formulas φ. We define P' as

$$P'(\pi) = \begin{cases} P(\pi') & \text{if } \pi = 0^{q(|P(\pi')|)}1\pi' \\ \varphi \vee \top & \text{if } \pi = (\varphi, \alpha) \text{ and } \alpha \text{ is a satisfying assignment for } \varphi \\ \top & \text{otherwise} \end{cases}$$

with some polynomial q such that $q(n) \geq \max\{|(\varphi, \alpha)| \mid |\varphi \vee \top| = n\}$. Obviously P' is a correct proof system with $P \equiv_p P'$. Furthermore $\mathrm{Ref}(P')$ is NP-complete because SAT reduces to $\mathrm{Ref}(P')$ via $\varphi \mapsto (\varphi \vee \top, 1^{q(|\varphi \vee \top|)})$.

For part 2 we define the proof system P as follows: (π, φ) is a P-proof of φ, if either π is a correct truth-table evaluation of φ with all entries 1, or φ is of the form $\psi \vee \top$ for some formula ψ and $\pi = 1^{\|\mathrm{Var}(\psi)\|}$.

The proof system P satisfies the condition $P \vdash_* \psi \vee \top$ for all formulas ψ. Hence by the proof of part 1 of this proposition there is a proof system P' with $P \equiv_p P'$ and NP-complete $\mathrm{Ref}(P')$. On the other hand the set $\mathrm{Ref}(P)$ is easily checked to be decidable in polynomial time. □

The second part of the above proposition tells us that the complexity of $\mathrm{Ref}(P)$ is not a robust property, i.e., it is not determined by the $\leq_p$-degree of the proof system P. For strong systems P simulating bounded-depth Frege systems we know that the set $\mathrm{Ref}(P)$ cannot be decided in polynomial time under cryptographic assumptions. Hence the exact characterization of the complexity of $\mathrm{Ref}(P)$ seems to be an interesting open problem. Are those sets candidates for languages with complexity intermediate between P and NP-complete?

Acknowledgements

For helpful conversations and suggestions on this work I am very grateful to Johannes Köbler, Jan Krajíček, and Pavel Pudlák. I would also like to thank the two anonymous referees for detailed comments on how to improve the paper. Author's research was supported by DFG grant KO 1053/5-1.

References

[1] A. Atserias, M.L. Bonet, On the automatizability of resolution and related propositional proof systems, in: Computer Science Logic, 16th International Workshop, 2002, pp. 569–583.
[2] M.L. Bonet, C. Domingo, R. Gavaldà, A. Maciel, T. Pitassi, Non-automatizability of bounded-depth Frege proofs, Computational Complexity 13 (1–2) (2004) 47–68.
[3] M.L. Bonet, T. Pitassi, R. Raz, Lower bounds for cutting planes proofs with small coefficients, The Journal of Symbolic Logic 62 (3) (1997) 708–728.
[4] M.L. Bonet, T. Pitassi, R. Raz, On interpolation and automatization for Frege systems, SIAM Journal on Computing 29 (6) (2000) 1939–1967.
[5] S.A. Cook, R.A. Reckhow, The relative efficiency of propositional proof systems, The Journal of Symbolic Logic 44 (1979) 36–50.
[6] C. Glaßer, A.L. Selman, S. Sengupta, Reductions between disjoint NP-pairs, Information and Computation 200 (2) (2005) 247–267.
[7] C. Glaßer, A.L. Selman, S. Sengupta, L. Zhang, Disjoint NP-pairs, SIAM Journal on Computing 33 (6) (2004) 1369–1416.
[8] C. Glaßer, A.L. Selman, L. Zhang, Canonical disjoint NP-pairs of propositional proof systems, in: Proc. 30th International Symposium on the Mathematical Foundations of Computer Science, 2005, pp. 399–409.
[9] J. Grollmann, A.L. Selman, Complexity measures for public-key cryptosystems, SIAM Journal on Computing 17 (2) (1988) 309–335.
[10] S. Homer, A.L. Selman, Oracles for structural properties: The isomorphism problem and public-key cryptography, Journal of Computer and System Sciences 44 (2) (1992) 287–301.
[11] J. Köbler, J. Messner, J. Torán, Optimal proof systems imply complete sets for promise classes, Information and Computation 184 (2003) 71–92.
[12] J. Krajíček, Bounded Arithmetic, Propositional Logic, and Complexity Theory, in: Encyclopedia of Mathematics and its Applications, vol. 60, Cambridge University Press, Cambridge, 1995.
[13] J. Krajíček, Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic, The Journal of Symbolic Logic 62 (2) (1997) 457–486.
[14] J. Krajíček, Dual weak pigeonhole principle, pseudo-surjective functions, and provability of circuit lower bounds, The Journal of Symbolic Logic 69 (1) (2004) 265–286.

[15] J. Krajíček, P. Pudlák, Propositional proof systems, the consistency of first order theories and the complexity of computations, The Journal of Symbolic Logic 54 (1989) 1063–1079.
[16] J. Krajíček, P. Pudlák, Quantified propositional calculi and fragments of bounded arithmetic, Zeitschrift für mathematische Logik und Grundlagen der Mathematik 36 (1990) 29–46.
[17] J. Krajíček, P. Pudlák, Some consequences of cryptographical conjectures for S_2^1 and EF, Information and Computation 140 (1) (1998) 82–94.
[18] L. Lovász, On the Shannon capacity of graphs, IEEE Transactions on Information Theory 25 (1979) 1–7.
[19] P. Pudlák, Lower bounds for resolution and cutting planes proofs and monotone computations, The Journal of Symbolic Logic 62 (1997) 981–998.
[20] P. Pudlák, On the complexity of propositional calculus, in: Sets and Proofs, Invited Papers from Logic Colloquium'97, Cambridge University Press, 1999, pp. 197–218.
[21] P. Pudlák, On reducibility and symmetry of disjoint NP-pairs, Theoretical Computer Science 295 (2003) 323–339.
[22] A.A. Razborov, On provably disjoint NP-pairs, Technical Report TR94-006, Electronic Colloquium on Computational Complexity, 1994.